

CLAIMS

We claim:

- 1 1. A method for manufacturing a trusted device comprising the steps of:
 - 2 (a) receiving keying information from a manufacturer, said manufacturer having
 - 3 received said keying information from a licensing authority;
 - 4 (b) generating a temporary private key;
 - 5 (c) computing a final private key using said temporary private key and said keying
 - 6 information;
 - 7 (d) computing a final public key using said temporary private key and said keying
 - 8 information;
 - 9 (e) sending said final public key to said manufacturer for certification; and
 - 10 (f) receiving a binding certificate from said manufacturer.
- 1 2. The method according to claim 1, wherein said keying information includes an initial
- 2 private key and a device identifier.
- 1 3. The method according to claim 2, further including the step of forgetting the initial
- 2 private key.
- 1 4. The method according to claim 1, further including the step of computing an
- 2 evidentiary certificate.
- 1 5. The method according to claim 4, wherein said evidentiary certificate includes text
- 2 and a signature of the text.

- 1 6. The method according to claim 4, further including the step of presenting a copy of
2 said evidentiary certificate to a second device.
- 1 7. The method according to claim 4, further including the step of said second device
2 verifying said evidentiary certificate.
- 1 8. The method according to claim 6, further including the steps of:
2 (a) said second device requesting a credential confirmation from said trusted
3 device;
4 (b) said trusted device computing a credential confirmation; and
5 (c) said trusted device presenting a copy of said credential certificate to said
6 second device.
- 1 9. The method according to claim 4, further including the step of presenting a copy of
2 said evidentiary certificate to said licensing authority.
- 1 10. The method according to claim 4, further including the step of said licensing authority
2 verifying said evidentiary certificate.
- 1 11. The method according to claim 10, wherein said step of said licensing authority
2 verifying said evidentiary certificate further includes the steps of:
3 (a) recomputing the final public key from the keying information and the
4 evidentiary certificate; and
5 (b) checking that the recomputed final public key with a manufacture's certificate.

1 12. The method according to claim 8, wherein said step of computing a credential
2 confirmation includes using a hash function.

1 13. An apparatus for manufacturing trusted devices comprising:

- 2 (a) a licensing authority for providing keying information;
- 3 (b) a multitude of manufactures, each of said manufactures receiving keying
4 information from the licensing authority; and
- 5 (c) a multitude of trusted devices, each of said trusted devices receiving keying
6 information from one of said multitude of manufacturers and generating a final
7 private trusted device key and final public trusted device key using the keying
8 information;

9 wherein said manufacture certifies said public trusted devices key.

1 14. An apparatus according to claim 13, wherein said licensing authority includes a
2 database, said database containing trusted device records.

1 15. An apparatus according to claim 14, wherein said trusted device records include a
2 public key.

1 16. An apparatus according to claim 14, wherein said trusted device records include:

- 2 (a) a trusted device identifier; and
- 3 (b) a manufacturer identifier.

1 17. An apparatus according to claim 14, wherein said set top box records include a set top
2 box public key.

1 19. An apparatus according to claim 14, wherein said trusted device records include a
2 communications identifier for identifying a device with which the trusted device may
3 communicate.